100

dvc		svr
102 ~ $\beta \leftarrow h(\pi)$		
104 ~ $\rho \leftarrow_R \{0,1\}^\lambda$		
106 ~ $\gamma \leftarrow E_{pk_{svr}}(<\beta, \rho>)$		
108 ~ $\delta \leftarrow \mathsf{mac}_a(<\gamma, \tau>)$		
	γ, δ, τ 110 →	
		$<a, b, c> \leftarrow D_{sk_{svr}}(\tau)$ ~ 112
		abort if $\mathsf{mac}_a(<\gamma, \tau>) \neq \delta$ ~ 114
		$<\beta, \rho> \leftarrow D_{sk_{svr}}(\gamma)$ ~ 116
		abort if $(\beta \neq b)$ ~ 118
		$\eta \leftarrow \rho \oplus c$ ~ 120
	η ← 122	
124 ~ $sk \leftarrow \rho \oplus \eta \oplus f(v, \pi)$		
126 ~ abort if $M(pk_{\mathsf{dvc}}, sk) \neq 1$		
128 ~ return sk		

FIG. 1

200

dvc		svr
202	$\beta \leftarrow h(\pi)$	
204	$\rho \leftarrow_R \{0,1\}^{\lambda}$	
206	$r \leftarrow_R \{0,1\}^{\kappa_{sig}}$	
208	$\gamma \leftarrow E_{pk_{svr}}(<m, r, \beta, \rho>)$	
210	$\delta \leftarrow \mathsf{mac}_a(<\gamma, \tau>)$	
	γ, δ, τ 212 →	
		$<a, b, u, d_2, N> \leftarrow D_{sk_{svr}}(\tau)$ 214
		abort if $\mathsf{mac}_a(<\gamma, \tau>) \neq \delta$ 216
		$<m, r, \beta, \rho> \leftarrow D_{sk_{svr}}(\gamma)$ 218
		abort if $\beta \neq b$ 220
		$\nu \leftarrow (\mathsf{encode}(m, r))^{d_2} \bmod N$ 222
		$\eta \leftarrow \rho \oplus \nu$ 224
	η ← 226	
228	$\nu \leftarrow \rho \oplus \eta$	
230	$d_1 \leftarrow f(v, \pi)$	
232	$s \leftarrow \nu(\mathsf{encode}(m, r))^{d_1} \bmod N$	
234	abort if $s^e \not\equiv_N \mathsf{encode}(m, r)$	
236	return $<s, r>$	

FIG. 2

300

dvc | **svr**

302 ~ abort if $\mathsf{valid}(c) = 0$

304 ~ $\beta \leftarrow h(\pi)$

306 ~ $\rho \leftarrow_R \{0,1\}^{\lambda+2|q|}$

308 ~ $\gamma \leftarrow E_{pk_{svr}}(<c, \beta, \rho>)$

310 ~ $\delta \leftarrow \mathsf{mac}_a(<\gamma, \tau>)$

γ, δ, τ $\longrightarrow$ 312

$<a, b, u, p, q, g, x_2> \leftarrow D_{sk_{svr}}(\tau)$ ~ 314

abort if $\mathsf{mac}_a(\gamma, \tau) \neq \delta$ — 316

$<c, \beta, \rho> \leftarrow D_{sk_{svr}}(\gamma)$ — 318

abort if $\beta \neq b \vee \mathsf{valid}(c) = 0$ — 320

$w \leftarrow \mathsf{select}(c)$ ~ 322

$\nu \leftarrow w^{x_2} \bmod p$ ~ 324

$r \leftarrow_R \mathbb{Z}_q$ ~ 326

$\nu' \leftarrow w^r \bmod p$ ~ 328

$e \leftarrow h_{\mathsf{zkp}}(<\nu, \nu', g^r \bmod p>)$ ~ 330

$s \leftarrow x_2 e + r \bmod q$ ~ 332

$\eta \leftarrow \rho \oplus <\nu, e, s>$ ~ 334

η $\longleftarrow$ 336

338 ~ $<\nu, e, s> \leftarrow \rho \oplus \eta$

340 ~ $w \leftarrow \mathsf{select}(c)$

342 ~ abort if $e \neq h_{\mathsf{zkp}}(<\nu, w^s \nu^{-e} \bmod p, g^s (y_2)^{-e} \bmod p>)$

344 ~ $x_1 \leftarrow f(v, \pi)$

346 ~ $\mu \leftarrow w^{x_1} \bmod p$

348 ~ return $\mathsf{reveal}(\nu\mu \bmod p, c)$

FIG. 3

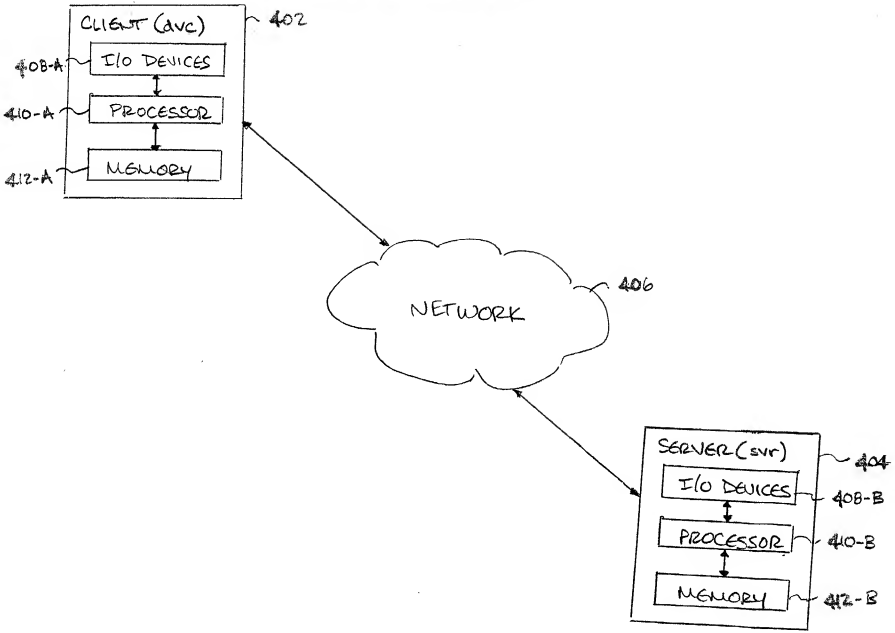
CLIENT (avc)
402
408-A
I/O DEVICES
410-A
PROCESSOR
412-A
MEMORY
NETWORK
406
SERVER (svr)
404
I/O DEVICES
408-B
PROCESSOR
410-B
MEMORY
412-B

FIG. 4